UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,737	08/03/2001	Fumihikko Sano	212288US2S	5068

22850 7590 09/22/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/920,737	SANO, FUMIHIKKO	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 19 July 2005. Claims 1-16 have been canceled. New Claims 17-53 have been added. Claims 17-53 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments with respect to claims 17-53 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

3. Claims 28, 29, 32, and 43-46 are objected to because of the following informalities:

Claim 28 refers to "The authenticating method according to claim 27", and Claims 43 and 44 refer to "The computer program according to claim 27". However, Claim 27 is directed to "An encryption/decryption method".

Claim 29 recites "a first program code" and "a third program code" but does not recite a second program code.

Claim 32 refers to "The computer program according to claim 31"; however, Claim 31 is directed to "An encryption/decryption method".

Claims 45 and 46 refer to "The encryption/decryption method according to claim 29"; however, Claim 29 is directed to "A computer program".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 17, 18, 21, 22, 25, 26, 29, 30, 33, 34, 37, 38, 41, 42, 45, 46, 49, 51, and 53 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 17 and 21 each recite the limitations "the first means for generating a plurality of key data by converting a common key using an intermediate result of a corresponding encryption function portion and a first type of conversion processing" and "the second means for generating a plurality of key data by converting the common key using an intermediate result of a corresponding encryption function portion and a second type of conversion processing". There is insufficient antecedent basis for these limitations in the claims. Further, the phrases appear to be missing language.

Claims 25 and 29 each recite the limitation "inputting at least one of the first and second key data to a subsequent encryption function processing that has not begun

processing". It is unclear what the subject of this limitation is; that is, it is not clear which process, function, code, or means performs the inputting.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claim 31 is rejected under 35 U.S.C. 102(e) as being anticipated by applicant admitted prior art.

Applicant discloses that the prior art teaches an encryption/decryption method including steps of outputting cipher text data by encrypting blocks of plain text data in parallel based on key data or outputting plain text data by decrypting blocks of cipher text data in parallel based on key data (Prior Art Figure 1, Encryption functions F), generating a plurality of key data including at least a first key data generated by converting a common key (Key K) based on an intermediate processing result of encryption or decryption processing on a preceding stage (i_1-i_{m-1} and s_1-s_{m-1}) and at

least a first type of conversion processing (Conversion functions f), and inputting the at least a first key data to encryption or decryption processing in a subsequent stage (see Figure 1).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 17-20, 25-28, 32-36, 41-44, 47-50, and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Johnson et al, US Patent 5796830.

In reference to Claims 17 and 19, and dependent Claims 18 and 20, Applicant discloses that the prior art teaches an encryption/decryption apparatus including a plurality of encryption function portions in parallel to each other which are used to encrypt plain text into cipher text or decrypt cipher text into plain text based on a key (Prior Art Figure 1, Encryption functions F) and a plurality of key data generating portions (or means) which generate key data by converting a common key (Key K) based on an intermediate processing result (i_1-i_{m-1} and s_1-s_{m-1}) and conversion processing (Conversion functions f). However, the admitted prior art does not explicitly disclose a first and second type of conversion processing, nor does it disclose

specifically that the first and second type of conversion processing convert the common key based on first and second variable data.

Johnson discloses a system in which a key is combined with a salt, which is a random variable used to increase randomness (column 12, lines 4-14). Johnson further discloses that a value to be encrypted can be divided into blocks, and a different salt chosen for each block (column 17, lines 42-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the encryption apparatus of the prior art to include converting a key based on a variable data, and by using different variable data to use more than one different type of conversion processing, in order to increase the randomness provided (see Johnson, column 12, lines 4-14).

Claims 25 and 26 are directed to a software implementation of the apparatus of Claims 17 and 18, and are rejected by a similar rationale.

Claims 27 and 28 are directed to methods corresponding substantially to the apparatus of Claims 17 and 18, and are rejected by a similar rationale.

In reference to Claim 32, the applicant admitted prior art discloses everything as applied to Claim 31 above. However, the admitted prior art does not explicitly disclose that the first conversion processing converts the common key based on a first variable data and the second conversion processing converts the common key based on a second variable data. Johnson discloses a system in which a key is combined with a

salt, which is a random variable used to increase randomness (column 12, lines 4-14). Johnson further discloses that a value to be encrypted can be divided into blocks, and a different salt chosen for each block (column 17, lines 42-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the encryption method of the prior art to include converting a key based on a variable data, in order to increase the randomness provided (see Johnson, column 12, lines 4-14).

In reference to Claims 33, 35, 41, 43, and 47, Johnson further discloses that the first type of conversion processing is based on a first function and the second type of conversion processing is based on a second function different from the first function (column 12, lines 4-14, and column 17, lines 42-60, where the different values of the salts, or random variables, make the conversion based on different functions).

In reference to Claims 34, 36, 42, 44, and 48, Johnson further discloses that the first and second type of conversion processing are based on a function, where the first type acts on a first bit position and the second type acts on a second bit position different from the first bit position (column 12, lines 4-14, and column 17, lines 42-60, where the different binary values of the salts make the functions act on different bit positions differently).

In reference to Claims 49, 50, and 53, Applicant further discloses that the prior art teaches that the first block of data on which encryption key data is based is the same

as the second block of data on which decryption key data is based (see Figure 1; page 2, lines 9-25 of the present specification).

10. Claims 21-24, 29, 30, 37-40, 45, 46, 51, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Johnson and further in view of Schneier, *Applied Cryptography*.

In reference to Claims 21 and 23, and dependent Claims 22 and 24, Applicant discloses that the prior art teaches an encryption/decryption apparatus including a plurality of encryption function portions in parallel to each other which are used to encrypt plain text into cipher text or decrypt cipher text into plain text based on a key (Prior Art Figure 1, Encryption functions F) and a plurality of key data generating portions (or means) which generate key data by converting a common key (Key K) based on an intermediate processing result (i_1-i_{m-1} and s_1-s_{m-1}) and conversion processing (Conversion functions f). However, the admitted prior art does not explicitly disclose a first and second type of conversion processing, nor does it disclose specifically that the first and second type of conversion processing convert the common key based on first and second variable data.

Johnson discloses a system in which a key is combined with a salt, which is a random variable used to increase randomness (column 12, lines 4-14). Johnson further discloses that a value to be encrypted can be divided into blocks, and a different salt chosen for each block (column 17, lines 42-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the

encryption apparatus of the prior art to include converting a key based on a variable data, and by using different variable data to use more than one different type of conversion processing, in order to increase the randomness provided (see Johnson, column 12, lines 4-14). However, neither the prior art disclosed by Applicant nor Johnson explicitly discloses generating an authenticator based on cipher text data generated by an encryption function.

Schneier discloses that a Message Authentication Code (MAC) can be generated using any keyed hash function such as a block cipher operating in cipher block chaining (CBC) mode (page 456, "CBC-MAC"). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the prior art encryption apparatus to be used in generating an authenticator such as a MAC, in order to provide authenticity without secrecy (see Schneier, page 455, section 18.14).

Claims 29 and 30 are directed to a software implementation of the apparatus of Claims 21 and 22, and are rejected by a similar rationale.

In reference to Claims 37, 39, and 45, Johnson further discloses that the first type of conversion processing is based on a first function and the second type of conversion processing is based on a second function different from the first function (column 12, lines 4-14, and column 17, lines 42-60, where the different values of the salts, or random variables, make the conversion based on different functions).

In reference to Claims 38, 40, and 46, Johnson further discloses that the first and second type of conversion processing are based on a function, where the first type acts on a first bit position and the second type acts on a second bit position different from the first bit position (column 12, lines 4-14, and column 17, lines 42-60, where the different binary values of the salts make the functions act on different bit positions differently).

In reference to Claims 51 and 52, Applicant further discloses that the prior art teaches that the first block of data on which encryption key data is based is the same as the second block of data on which decryption key data is based (see Figure 1; page 2, lines 9-25 of the present specification).

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER